United Nations

FCCC/SBI/2015/INF.2

Framework Convention on
Climate Change

Distr.: General
9 April 2015

English only

Subsidiary Body for Implementation
Forty-second session
Bonn, 1–11 June 2015

Item 5(e) of the provisional agenda
Matters relating to the mechanisms under the Kyoto Protocol
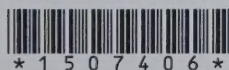**Matters relating to the international transaction log under the Kyoto Protocol**

Information security implementation in registry systems

Note by the administrator of the international transaction log

Summary

       Subsequent to preliminary efforts of the international transaction log (ITL) administrator and the Security Working Group established under the Registry System Administrators Forum, this document specifies the implementation status of information security controls in registry systems. This document also presents the recommended security implementation actions and their related resource requirements. The Subsidiary Body for Implementation may wish to take note of the information contained in this document and provide guidance to the ITL administrator and Parties, as necessary, concerning the information security implementation in registry systems.

Please recycle

Contents

I.   Introduction

A.   Mandate

1.   The Conference of the Parties, by decision 24/CP.8, and the Conference of the Parties serving as the meeting of the Parties to the Kyoto Protocol (CMP), by decisions 3/CMP.1 and 13/CMP.1, requested Parties included in Annex B to the Kyoto Protocol to establish and maintain a national registry in order to ensure the accurate accounting of transactions of Kyoto Protocol units. Furthermore, the CMP requested the secretariat to establish and maintain an international transaction log (ITL) in order to verify the validity of the transactions proposed by registries. The ITL and registry systems are essential for the implementation of the mechanisms under Articles 6, 12 and 17 of the Kyoto Protocol.

2.   The CMP, by decision 12/CMP.1, requested the Subsidiary Body for Implementation (SBI) to consider, at its future sessions, the annual reports of the ITL administrator, with a view to requesting the CMP to provide guidance in relation to the operation of registry systems.

3.   The eighth annual report of the ITL administrator[1] provided recommendations to CMP 8 based on lessons learned during the first commitment period of the Kyoto Protocol. In these recommendations, it was proposed that information security management be improved based on the International Organization for Standardization/the International Electrotechnical Commission (ISO/IEC) 27001[2] and ISO/IEC 27002[3] standards.

4.   In order to assess the impact of managing information security on the basis of ISO/IEC standards, the ITL administrator established a Security Working Group (SWG) under the Registry System Administrators Forum. Following the definition of objectives and plans to adopt a framework for managing the security of the information assets within registry systems, the ITL administrator and the SWG identified relevant assets and their associated information security requirements, reviewed known information security threats, and selected relevant controls in order to manage risks.

5.   SBI 40 continued the consideration of information security management in registry systems. It welcomed the document prepared by the ITL administrator and the SWG and took note of the options for, and road map to, information security implementation in the registry system.[4] In this document, the ITL administrator and the SWG identified two options for facilitating the implementation of supplementary security controls in registry systems. These were the business as usual and further implementation options.

6.   SBI 40 requested the ITL administrator and the SWG to execute the further implementation option by extending the current information security control implementation on the basis of a registry-specific and quantitative risk assessment, followed by an in-depth control implementation analysis. It also requested the ITL administrator and the SWG to prepare a document containing a final implementation option for information security management, including the related resource requirements for registry systems and the budget requirements for the ITL, for consideration at SBI 42.[5]

---

[1]   FCCC/KP/CMP/2012/8, paragraph 58(b).

[2]   ISO/IEC 27001:2013. Security techniques – Information security management systems – Requirements.

[3]   ISO/IEC 27002:2013. Security techniques – Code of practice for information security controls.

[4]   FCCC/SBI/2014/INF.6.

[5]   FCCC/SBI/2014/8.

B. Scope of the note

7. This document includes an analysis by the ITL administrator and the SWG of the current implementation status of the security controls in registry systems. This analysis contains the following:

(a) The scope of the registry-specific and quantitative risk assessment, which elaborates on the security questionnaire provided to national registries;

(b) The status of information security control implementation, as assessed by the ITL administrator and the SWG, based on the analysis of responses to the security questionnaire;

(c) The recommendations related to developing and establishing arrangements for the implementation of further information security controls in registry systems;

(d) The anticipated resource requirements and the timeline for the implementation of the recommendations, for consideration at SBI 42.

C. Possible action by the Subsidiary Body for Implementation

8. The SBI may wish to take note of the information included in this report, and determine further action to be taken by the ITL administrator and the administrators of other registry systems concerning information security implementation in registry systems.

II. Possible implications of implementation of further information security controls in registry systems

A. General considerations

9. Information security is focused on the protection of the **confidentiality**, **availability** and **integrity** of information. Information security is achieved by implementing a suitable set of controls. These controls include a range of activities related to policies, processes, procedures, organizational structures, software and hardware. The application of controls that effectively treat and manage risks is based on risk assessment.

10. Currently, the data exchange standards (DES),[6] established and maintained in accordance with decision 24/CP.8, mandate a set of security controls that are applied to data exchange between the ITL and registry systems. A central review of the controls specified in DES is carried out by the ITL administrator when establishing a registry's readiness to connect to the ITL. Changes in the application of these controls are assessed during the standard independent assessment report (SIAR) process pursuant to decision 16/CP.10, the results of which are forwarded for consideration by expert review teams under Article 8 of the Kyoto Protocol. In addition to the controls contained in DES, registry system administrators (RSAs) can apply additional security controls on a voluntary basis.

---

[6] The latest version is available at:
<http://unfccc.int/files/kyoto_protocol/registry_systems/itl/application/pdf/data_exchange_standards_for_registry_systems_under_the_kyoto_protocol.pdf>.

B.   Scope of the registry specific and quantitative risk assessment

11.   The scope of an in-depth, registry specific and quantitative risk assessment included security controls within the context of the business processes and information systems that enable emissions trading in registry systems.

12.   The ITL administrator and the SWG prepared a security questionnaire which was provided to 38 national registries in October 2014. Twenty-six RSAs responded to the questionnaire by December 2014. Questions specific to the Consolidated System of European Union Registries (CSEUR) were answered by the European Commission on behalf of the Parties participating in the CSEUR.

13.   Based on the responses to the security questionnaire, the ITL administrator and the SWG analysed the implementation status of information security controls as specified in the following 11 control categories from the ISO/IEC 27002 international standard:

(a)   Administrative information security policy controls which provide direction and support for information security, in accordance with business and legal requirements, and initiate the implementation and operation of information security within registry systems;

(b)   Human resource security controls which ensure that staff and contractors understand their responsibilities;

(c)   Asset management controls which direct the identification of classified assets and define appropriate protection responsibilities;

(d)   Access controls which limit access to information and information processing facilities;

(e)   Cryptography controls which ensure proper and effective use of cryptography in order to protect the confidentiality, authenticity and/or integrity of information;

(f)   Physical and environmental security controls which prevent unauthorized physical access and damage to as well as interference with information and information processing facilities;

(g)   Operations security controls which ensure secure operations in registry systems;

(h)   System development, acquisition and maintenance controls which ensure that information security is an integral part of the entire information system's life cycle;

(i)   Supplier relationship controls which ensure protection of the assets that are accessible by suppliers;

(j)   Information security incident management controls which ensure a consistent and effective approach to the management of information security incidents;

(k)   Business continuity management controls which ensure that information security is embedded in the organization's business continuity plans and processes.

14.   Questions related to controls contained in DES were not included in the questionnaire, as they are already implemented through DES and the SIAR process.

C.   Assessment of information security controls implementation status

15.   Based on the analysis of responses to the security questionnaire, the ITL administrator and the SWG concluded that a range of supplementary controls have been
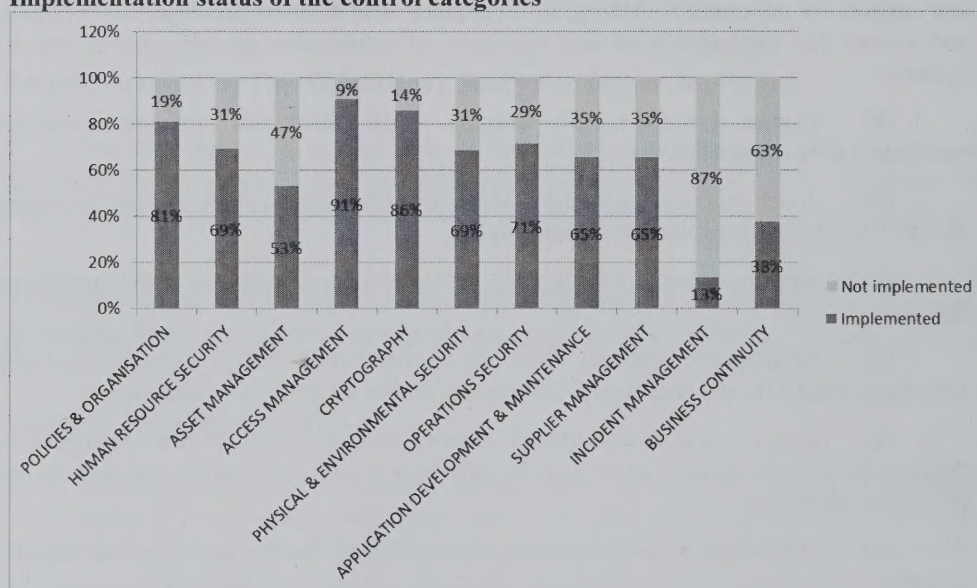
applied based on the initiative of national registries. As is evident from the responses, most RSAs already apply an established management framework, which includes activities to:

(a)　　Initiate and control the implementation and operation of information security within registry systems;

(b)　　Limit or prevent access to national registry information assets;

(c)　　Ensure proper and effective use of cryptographic means in order to protect the confidentiality and integrity of information;

(d)　　Ensure correct and secure operations of information processing facilities;

(e)　　Ensure that information security is an integral part of information systems.

16.　　The implementation status of the control categories across all respondents is represented in the figure below.

Figure
Implementation status of the control categories

17.　　In March 2015, the ITL administrator provided registry-specific feedback to each responding national registry, based on the responses to the questionnaire. This feedback included references to the control categories that are reported as implemented by RSAs. In addition, the feedback included a specific risk assessment and corresponding recommendations regarding controls incompletely implemented in a national registry.

18.　　Based on an overall analysis of the responses to the security questionnaire, the ITL administrator and the SWG identified asset management, information security incident management and security aspects of business continuity management as the control categories with the most significant implementation gaps across national registries.

D.　Recommendations for implementation of further information security controls

19.　　Decision 16/CP.10, paragraph 4, provides the mandate to the ITL administrator, in cooperation with administrators of other registry systems, to develop common operational procedures for implementation in all registry systems, as well as recommended practices

and information-sharing measures for registry systems, in order to facilitate and promote compatibility, accuracy, efficiency and transparency in the operation of registry systems.

1. Asset management

20.   To rationalize security efforts in registry systems, it is suggested that the ITL administrator, in cooperation with administrators of other registry systems, develops, establishes and maintains requirements for managing inventories, related to information assets under the control of RSAs, which are of value to emissions trading under the Kyoto Protocol.

21.   The information asset inventory defines the necessary structures that allow for the protection of particular assets. It includes digitized and physical, and tangible and intangible information technology service and human-related data. The information asset inventory further specifies assets' relative business value, their type and format, location, classification and ownership.

22.   The individual asset inventories, implemented and managed by administrators of registry systems, should define the levels of protection corresponding to the value as well as the importance of the assets.

2. Information security incident handling

23.   It is further suggested that the ITL administrator, in cooperation with administrators of other registry systems, reviews and updates the common operational procedure for the handling of security incidents.

24.   The procedure for the handling of security incidents should be updated in order to include incident detection, incident communication to potentially impacted stakeholders, incident evaluation as well as prioritization and incident response. The updated procedure should enable the resolution of any actual, suspected or potential breach of confidentiality, availability or integrity of information assets recorded by registry systems in their information asset inventory referred to in paragraphs 20–22 above.

3. Information security aspects of business continuity management

25.   The initialization process, included in DES, describes the process of bringing a registry system online, and allowing it to connect to the ITL and become fully operational. Prior to participating in a message exchange with the ITL, the registry must comply with a series of initialization requirements and procedures. This includes a disaster recovery plan designed to ensure business continuity in the event of catastrophic failure or disruption of the host environment.

26.   Based on the responses to the security questionnaire, 63 per cent of the responding national registries reported that they do not establish, document, implement or maintain business continuity controls or only do so partially.

27.   It is suggested that the ITL administrator reassesses changes in business continuity plans of the national registries which reported an incomplete implementation of the controls in these plans. This reassessment would ensure that the required level of information security continuity is maintained in the registry environments and would be conducted in conjunction with the SIAR process.

E. Resource requirements and the implementation timeline

28.   The actions to be performed by the ITL administrator as a result the suggested recommendations can be accommodated within the ITL budget. An estimated implementation time of several months is anticipated. Reassessment of the changes in business continuity plans of the national registries can be completed in the annual SIAR process in 2016.

29.   The ITL administrator and the SWG are not in a position to estimate the resource requirements or the implementation time required by RSAs to establish their arrangements for implementing the specified recommendations, owing to their national circumstances and organizational arrangements.

_____